



THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

AUG 18 2010

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Final Recommendations of the Ft. Hood Follow-on Review

The tragic shooting of U.S. military personnel at Fort Hood in November 2009 underscored the need for the DoD to thoroughly review its approach to force protection and to broaden its force protection policies, programs, and procedures to go beyond their traditional focus on hostile external threats. I commissioned the DoD Independent Review Related to Fort Hood to assist the Department in identifying existing gaps and deficiencies, and also to help broaden the Department's force protection approach to reflect more effectively the challenging security environment in which we operate.

I have carefully considered the recommendations in the Independent Review's report, *Protecting the Force: Lessons Learned from Fort Hood*, and am directing that the Department respond to them by taking appropriate action, as specified in the attached final report of the DoD Follow-on Review to the Fort Hood incident. In a small number of cases, further study will be required before the Department can take additional steps. For the majority of recommendations, however, the Follow-on Review recommends concrete actions. The Department will make every effort to safeguard civil liberties as it develops these policies and programs.

These initiatives will significantly improve the Department's ability to mitigate internal threats, ensure force protection, enable emergency response, and provide care for victims and families. In particular, the Department will strengthen its policies, programs, and procedures in the following areas:

- Addressing workplace violence;
- Ensuring commander and supervisor access to appropriate information in personnel records;
- Improving information sharing with partner agencies and among installations;
- Expanding installations' emergency response capabilities;
- Integrating force protection policy, and clarifying force protection roles and responsibilities; and



OSD 07688-10

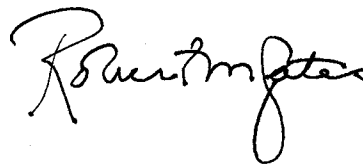


Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 2010		2. REPORT TYPE		3. DATES COVERED 00-00-2010 to 00-00-2010	
4. TITLE AND SUBTITLE Final Recommendations of the Ft. Hood Follow-on-Review				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The Secretary of Defense,1000 Defense Pentagon,Washington,DC,20301-1000				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 26	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

- Ensuring that we provide top quality health care to both our service members and our healthcare providers.

I expect Department leaders to place great priority on implementing these recommendations. To ensure the Department maintains an enduring focus on eliminating the gaps and deficiencies identified in *Protecting the Force*, I am directing that the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD&ASA)) continue to lead the Fort Hood Follow-on Review as it transitions its focus to monitoring implementation of the actions directed in this memorandum. The ASD(HD&ASA) will provide regular implementation progress reports to me, not only on those measures that I have approved, but also on progress by Military Department Secretaries and Combatant Commanders to mitigate issues identified in their independent internal reviews. The ASD(HD&ASA) will continue in this role until such point that he advises that implementation of each recommendation is sufficiently underway to render further monitoring unnecessary.

Force protection, although critical, is not a substitute for leadership. Leaders at every level in our military play a critical role. Leading forces is both a duty and a privilege, and it carries with it the clear responsibility to ensure good order and discipline. Leaders must be prepared to intervene when necessary; poor performance should never be ignored. The Department will continue to enable military leaders with the tools and discretion they need to take appropriate action to prevent and respond to potential problems, whatever their cause. As the Department takes steps to strengthen its approach to force protection, I ask leaders and commanders across the force to remain mindful of the unique requirements of the profession of arms – that military service is grounded in an oath to support and defend our Constitution, but also may necessitate the sacrifice of some of the very rights we defend. Our all-volunteer force reflects the strength of our national diversity and is composed of patriots who are first and foremost Soldiers, Sailors, Airmen, or Marines sworn to uphold our national values.



Attachment:
As stated

DISTRIBUTION:

**SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF THE MILITARY SERVICES
COMMANDERS OF THE COMBATANT COMMANDS
CHIEF OF THE NATIONAL GUARD BUREAU
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES**

**Department of Defense Implementation of Recommendations
from the Independent Review Related to Fort Hood**

Recommendation 2.1 a-d: Update Policies and Develop Programs to Identify Behavioral Indicators of Violence

The Independent Review found that DoD programs, policies, processes, and procedures that address identification of indicators for violence and radicalization are outdated, incomplete, and fail to include key indicators of potentially violent behaviors. There is no risk assessment system available to supervisors and commanders to help them identify and mitigate internal threats. Such a system must be developed to provide supervisors and commanders with better tools to identify internal threats, recognize when to intervene, and make judgment calls in disciplinary cases and when conducting performance and career counseling.

- **Future Action to Identify Behavioral Indicators of Violence:** The Department will take a 3-step approach to provide commanders and supervisors with the information and tools needed to identify and respond to internal threats. First, the Department will issue commanders and civilian supervisors interim guidance on how to identify internal threats.
- Second, the Department will conduct three formal studies to deepen our understanding of internal threats and refine the guidance contained in the interim message. By March 2011, the Defense Science Board (DSB) will identify behavioral indicators of violence and radicalization, develop threat assessment methodologies, and investigate optimal insider threat training delivery methods. In addition, OASD (HA) will conduct two scientific studies, one retrospective and one prospective, that will examine DoD populations and develop a scientifically based list of behavioral indicators of potential violence. The Follow-On Review Senior Steering Group will also coordinate with the FBI Behavioral Science Unit to further strengthen our understanding of insider threat.
- Third, the Under Secretary of Defense for Personnel and Readiness (USD (P&R)) and the Under Secretary of Defense for Intelligence (USD(I)) will integrate the Department's findings into existing programs no later than September 2011. Results from longer-term, ongoing studies will be integrated into policies and programs as appropriate upon study completion.

Recommendation 2.2 a-d: Review Personnel Policies for Access to Installations and Information

The Independent Review found that background checks on civilians entering the military or DoD civilian workforce may be incomplete, too limited in scope, or not conducted at all. The Independent Review also found that guidelines for adjudicating security clearances are vague, and training on how and to whom significant information reports are made is insufficient. Successful implementation of Homeland Security Presidential Directive-12 (HSPD-12), a government-wide standard for reliable identification verification, will mitigate current risk assumed by DoD. It mandates that all employees requiring a DoD Common Access Card (CAC) undergo, at a minimum, a National Agency Check with Inquiries prior to receiving a CAC. Some employee populations (i.e., temporary or seasonal hires) are not subject to mandatory

background investigations under HSPD-12. Further mitigating risk, the interagency Joint Reform Team (JRT) made recommendations to reform federal investigative standards, including revising the scope of the National Agency Check with Local Agency (NACLC) and aligning suitability for employment with national security.

The JRT effort to revise the scope of the NACLC renders unnecessary the Independent Review recommendation to review the appropriateness of the NACLC as a minimum background investigation for a DoD SECRET clearance. In addition, the Follow-on Review found no evidence that legal advisors lack understanding of the adjudicative guidelines or that the guidelines are vague, negating the need for additional specialized training.

- **Future Action to Strengthen Installation Access Policies:** The Under Secretary of Defense for Intelligence (USD(I)), in consultation with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), will revise DoDI 5200.02 and DoDM 5200.02 (currently both in draft form with the title *Personnel Security Program*) to comply with HSPD-12 mandates and JRT reform efforts no later than September 2011. Additionally, USD(I) will develop a plan to ensure the widest dissemination of *Roles and Responsibilities for Personnel Security: A Guide for Supervisors* throughout DoD so commanders and supervisors have access to this information. USD(P&R) will publish policy designating which individuals not covered by HSPD-12 should receive background investigations. USD(P&R) will also review current policy regarding expedited citizenship for certain classes of workers and make recommendations for updates by December 2010. The Department is projected to be in full HSPD-12 compliance by the end of CY 2012.

Recommendation 2.3: Recognition of Individuals as Ecclesiastical Endorsers of Chaplains

The Independent Review found that DoD standards for denying requests from organizations that want recognition as an ecclesiastical endorser are inadequate. An ecclesiastical endorser issues and withdraws credentials given to individuals to perform religious services in accordance with the practice of the granting organization. DoD Instruction (DoDI) 1304.28 (Guidance for the Appointment of Chaplains for the Military Departments) provides the Department with broad authority to deny recognition to individuals as ecclesiastical endorsers while also ensuring the ability of military members to exercise freedom of religion. Although this policy is appropriate, the Department will review and update existing policy to ensure effective implementation, including periodic reviews of religious organizations seeking to endorse religious ministry professionals as military chaplains.

- *The Under Secretary of the Defense for Personnel and Readiness will review DoDI 1304.28 to ensure it includes effective implementation procedures, and update the instruction as appropriate by September 2010.*

Recommendation 2.4: Establish Rigorous Procedures for Investigating Foreign National DoD Personnel

The Independent Review found that a number of populations presently granted physical access to DoD facilities overseas require some form of vetting for repeated access. Some notionally vetted populations have incomplete records, and large numbers of people with access to DoD facilities are not vetted at all under current procedures.

DoD's ability to investigate foreign national DoD employees who live outside of the U.S. and require access to DoD facilities is limited by available resources and agreements with the host nation. DoD is only able to conduct the FBI name check, fingerprint check, and a check of the known and suspected terrorist databases. The Government Accountability Office (GAO) Report 09-351, *Contingency Contract Management*, highlights issues in complying with DoD 5200.2-R (*Personnel Security Program*). Additionally, compliance with Homeland Security Presidential Directive 12 requires background investigations for foreign national hires, or the equivalent host nation review, for access to DoD installations.

- **Future Action to Investigate Foreign National Employees:** By September 2010, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), in collaboration with the Under Secretary of Defense for Intelligence (USD(I)), the Under Secretary of Defense for Policy (USD(P)), and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will comply with existing relevant policy issuances (DoD 5200.2-R, DTM 08-003, and DTM 06-006) by developing relevant programs or identifying policy issues for discussion and implementation. USD(AT&L), as the lead to develop a response to GAO Report 09-351, will provide a summary of possible improvements not later than December 2010. By February 2011, USD(I), USD(P&R), and USD(AT&L) will revise applicable policy issuances to reflect the agreed-upon process and improvements. The Fort Hood Follow-on Review Senior Steering Group will monitor responses and require reports in consultation with the DoD Inspector General.

Recommendation 2.5 a-c: Review Pre- and Post-Behavioral Screening

The Independent Review found that the policies and procedures governing assessment for pre- and post-deployment medical risks do not provide a comprehensive assessment of violence indicators. There is no global violence risk assessment performed during pre-deployment for service members not currently receiving healthcare.

Current post-deployment assessments rely primarily on self-report screening questionnaires to identify risk factors for post-traumatic stress, traumatic brain injury, substance abuse, depression, and suicide. These screening questionnaires often ask just one question to assess whether a service member has serious conflict with others. A follow-up provider interview directs medical providers to conduct a risk assessment by asking whether members are considering harm to self or others. However, the assessments do not address all risk factors (e.g., financial, occupational) thought to be associated with the potential for violence. Research-based screening questions do not exist and there is no current ability to reliably predict violence or a proclivity towards radicalization.

- **Future Action to Improve Behavioral Screening:** The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will conduct several studies to inform pre- and post-deployment assessments and refine DoD behavioral indicators ("Step 2" of Recommendation 2.1). Additionally, USD(P&R) reviewed scientific literature and conducted interviews with subject matter experts to identify indicators for measuring an individual's potential for future violence and to determine whether an evidence-based comprehensive risk assessment system exists. Based on the literature review, which was completed in June 2010, USD(P&R) will adjust the policy guidance for serial mental health assessments required by the National Defense Authorization Act 2010, to include an additional service member question relating

to factors that have been correlated with violence (i.e., work, home, financial, legal, and interpersonal stressors). In addition, the guidance for health care providers will include detailed follow-up questions for the assessment of violence risk and indications for referral.

- The final policy for implementing mental health assessments will be issued no later than August 2010; the final guidance for training and certifying providers to do the assessments will be issued no later than September 2010. USD(P&R) is also developing partnerships with organizations with expertise in risk management to determine any lessons that may apply to DoD.

Recommendation 2.5.d: Review Policies Governing Sharing Health Care Assessments with Commanders

The Independent Review found that appropriate commanders, supervisors, and other authorities do not always receive information about individuals who may commit violent acts because they may not have sufficient access to health care assessments. A significant body of policies already exists within DoD to ensure that commanders and supervisors do receive appropriate health care-related information about their subordinates. However, these policies are spread across multiple regulations, memoranda, and instructions. A number of these policies have not been reviewed in more than 10 years and may need to be updated.

- *The Under Secretary of Defense for Personnel and Readiness will review existing policies and guidance to evaluate their content, and update them as necessary by September 2010.*

Recommendation 2.6 a, b: Update Policies to Address Workplace Violence

The Independent Review found that the Services have programs and policies to address prevention and intervention for suicide, sexual assault, and family violence, but guidance concerning workplace violence and the potential for self-radicalization is insufficient. These programs may serve as useful resources for developing more comprehensive workplace violence prevention—including the potential for self-radicalization. Useful resources for violence prevention education and training also exist in other federal agencies but are dated and not integrated into DoD policies, procedures, or processes.

- **Future Action to Address Workplace Violence:** The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will develop DoD policy and guidance on the prevention of workplace violence by January 2011. USD(P&R) will incorporate training on prevention of workplace violence into the Civilian Personnel Management Services' Managerial and Supervisory Training Framework in accordance with the requirements of the National Defense Authorization Act FY2010 Section 1113.

Recommendation 2.7: Update Policy to Clarify Guidelines for Religious Accommodation

The Independent Review found that DoD policy regarding religious accommodation lacks the clarity necessary to help commanders distinguish appropriate religious practices from those that might indicate a potential for violence or self-radicalization. DoDI 1300.17 (*Accommodation of Religious Practices within the Military Services*) outlines the terms upon which religious

accommodations should be granted, but it does not provide standards or record keeping procedures necessary to establish a baseline of traditional religious practice within faith groups. Therefore, Services have different policies and procedures for handling religious accommodation requests. Further, DoD has not issued clear guidance on the degree to which the Religious Freedom Restoration Act (RFRA) applies to the military. The Independent Review recommended the Department promptly establish standards and reporting procedures that clarify guidelines for religious accommodation.

➤ **Future Action to Establish Standards and Clarify Guidelines for Religious**

Accommodations: The Independent Review raised an important, long-standing concern and the Department agrees there is a need for consistent and overarching policy to standardize the religious accommodation approval process. The Undersecretary of Defense for Personnel and Readiness will work with the Services to examine this issue in more detail and, when appropriate, will provide a recommendation to the Secretary.

Recommendation 2.8: Provide Guidance for Counterintelligence Awareness

The Independent Review found that DoDI 5240.6 (Counterintelligence (CI) Awareness, Briefing, and Reporting Programs) provides guidance to conduct defense CI and counter-terrorism awareness briefings to DoD personnel, but does not thoroughly address emerging threats, including self-radicalization, which may contribute to an individual's potential to commit violence.

- *By September 2010, the Under Secretary of Defense for Intelligence will begin formal coordination of DoDI 5240.6, updated with a list of potential behavioral indicators with a nexus to international terrorism and language directing CI entities to disseminate other reported behaviors to command authorities and/or to law enforcement agencies. By September 2010, the Under Secretary of Defense for Policy will work with the Defense Science Board to undertake a multi-disciplinary study to identify behavioral indicators of violence and self-radicalization and update DoDD 2000.12 (DoD Antiterrorism (AT) Program), DoDO 2000.12-H (DoD Antiterrorism Handbook), and DoDI 2000.16 (DoD Antiterrorism (AT) Standards) as appropriate.*

Recommendation 2.9 a, b: Update Policies to Ensure Commander and Supervisor Access to Information in Personnel Records

The Independent Review found that neither DoD nor Service guidance provides for the maintenance and transfer of all relevant information about service members' conduct throughout their careers. At present, only performance evaluations (the Official Military Personnel Folder (OMPF)) and medical records follow service members across all assignments. DoDI 1336.08 (*Military Human Resource Records Life Cycle Management*) governs the type of records to retain and DoDI 6040.43 (*Custody and Control of Outpatient Medical Records*) requires that all treatment records be maintained for medical, legal, and administration reasons. Gaining commanders and supervisors would benefit from additional visibility into service members' behavior, especially that which may undermine good order and discipline or indicate a potential insider threat to DoD and its personnel.

In March 2010, the Human Resources Management Community of Interest established the Military Personnel Records Information Management Task Force (MPRIMTF) to examine the need to maintain and share additional information in personnel records. In May 2010, MPRIMTF completed its review and concluded that no additional information should be added to the OMPF. Although the MPRIMTF found that the OMPF is not the appropriate vehicle to maintain and share additional information, the Task Force does affirm that the Department must ensure commanders have more visibility into service members' behavior.

Future Action to Ensure Access to Information in Personnel Records: The Secretary of Defense will issue a memorandum to the Chiefs of the Military Services, directing them to determine procedures for appropriate documentation of behaviors detrimental to good order and discipline, particularly those that could be associated with violence, prohibited activities, and potential harm to self or others. The procedures should increase engagement of unit commanders and supervisors to prevent potential acts of violence and ensure timely and appropriate support for military personnel in need. These new procedures must be consistent with the Privacy Act and DoDD 5400.11 (*DoD Privacy Program*). Service Chiefs are requested to inform the Secretary of their proposal within 30 days.

Recommendation 2.10: Establishment of Consolidated Law Enforcement Database

The Independent Review recommended establishing a consolidated database to enable organizations across the Department to query, retrieve, and post criminal investigation and law enforcement data in a single repository. In August 2008, the Secretary of Defense directed that the existing Naval Criminal Investigative Service system be used as the basis for establishing a consolidated Law Enforcement Defense Data Exchange (D-DEx). Each of DoD's thirteen law enforcement agencies are *participating in the development of D-DEx*.

- *The Under Secretary of Defense for Personnel and Readiness, in coordination with the Military Departments and other Defense Law Enforcement Agencies, will complete development of D-DEx and identify program funds to deploy D-DEx DoD-wide in FY2011.*

Recommendation 2.11: Establish Formal Information Sharing Agreements with Partner Agencies

The Independent Review found that existing DoD guidance on establishing information sharing agreements with Federal, State, and local law enforcement and criminal investigation organizations does not mandate action or provide clear standards. The Independent Review recommended the Department require the Military Departments and Defense Agencies to establish formal information sharing agreements with allied and partner agencies; Federal, State, and local law enforcement; and criminal investigation agencies, with clearly established standards regarding scope and timeliness. The report noted that a lack of information sharing with partners reduces commanders' and supervisors' visibility into service members' conduct off-installation and renders them less able to identify and respond to potential insider threats.

The Follow-On Review found that not all information sharing relationships will be improved through formal agreements. At the local and international level, current information sharing policies and procedures are adequate. Attempts to formalize these information sharing relationships will be counterproductive, since this approach would convey a lack of trust and

reduce partners' incentives to cooperate by increasing their administrative and legal burdens. Therefore, the Follow-On Review found that the Department could benefit from formal agreements for a limited set of force protection threat information sharing relationships.

- **Future Action to Strengthen Information Sharing with Partners:** By September 2011, the Follow-On Review Senior Steering Group will appoint a lead agency to develop DoD guidance requiring formal agreements with: (a) U.S. Federal Department or Agencies, or any subsidiary organization; (b) Office of the Director of National Intelligence or any subsidiary organization; and (c) U.S. State, Territorial, or Tribal governments.

Recommendation 2.12: Update Policies on the Release of Protected Health Information

The Independent Review found that Service policies governing release of protected health information do not reflect current DoD-level guidance. Release of protected health information in DoD is governed by Privacy Regulations issued under the Health Insurance Portability and Accountability Act, which balances confidentiality with the need to ensure operational readiness and is reflected in DoD- and Service-level policy. DoD has recently provided interim guidance that indicates the circumstances under which it is appropriate and required for a healthcare provider to release protected health information to commanders. However, not all current Service-level guidance has been updated to reflect the most recent DoD policy.

- **Future Action on Protected Health Information:** The Under Secretary of Defense for Personnel and Readiness will direct the Secretaries of the Military Departments to review existing policies and guidance and update them as necessary to reflect DoD policy on the release of protected health information by September 2010. The Services will ensure that updated policy reflects the anti-stigma DoDI to be placed into coordination by September 2010, currently under conversion from DTM 09-006 (*Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel*).

Recommendation 2.13: Adopt Policies to Ensure Timely Dissemination of Violence Risk Assessments from Civilian Health Professionals to Military Personnel

The Independent Review found that current policy does not require civilian health professionals who provide care to service members to notify military health treatment facilities or commanders of indicators of violence that are identified during treatment. This gap in visibility prevents military medical providers, commanders, and supervisors from assisting the service member or intervening until the risk indicators result in observable behaviors that trigger concern.

- **Future Action to Disseminate Violence Risk Assessments:** The Under Secretary of Defense for Personnel and Readiness will review policies and procedures to ensure that appropriate information (i.e., information on a service member's threat of harm to self or others, or a diagnosis that involves treatment requiring duty limitations) from civilian providers to whom service members have been referred from the Military Health System may be provided to commands and military medical personnel. Appropriate policy guidance to Services will be drafted and placed into coordination by September 2010.

Recommendation 2.14: Publish Cyberspace Policy for Identifying Potential Threats to DoD Personnel, Information, and Facilities

The Independent Review found that the Department does not have a comprehensive and interagency-coordinated cyberspace counterintelligence (CI) activities policy. DoD has started drafting DoDI 5240.mm to address this shortfall. This interagency coordinated policy will provide comprehensive guidance for CI activities in cyberspace to all Military Departments and Defense Agencies. This policy will not address law enforcement activities but will compel defense CI components to alert DoD investigative organizations of non-foreign intelligence threat information discovered during authorized CI activity.

- *The Under Secretary of Defense for Intelligence in coordination with all interagency partners will publish DoDI 5240.mm by August 2010 to ensure DoD CI activities in cyberspace effectively counter espionage and support force protection.*

Recommendation 2.15: Prohibited Activities

The Independent Review found that DoD policy governing prohibited activities is unclear and does not provide commanders and supervisors the guidance and authority to act on potential threats to good order and discipline. DoD policy on prohibited activities is limited and only addresses active participation in groups that may pose threats to good order and discipline. Current DoD policy on prohibited activities appropriately balances personal expression against actions that undermine good order and discipline. DoDI 1325.06 (Handling Dissident And Protest Activities Among Members of the Armed Forces) and Article 134, Uniform Code of Military Justice, define actions that are detrimental to good order and discipline and empowers commanders to act in these instance. However, further clarification is necessary to illustrate more effectively what constitutes associational, advocating, supremacist and extremist behavior.

- *The Under Secretary of the Defense for Personnel and Readiness will review DoDI 1325.06 to ensure guidance is actionable and to provide behavior examples, guidance on how to respond to uncertain situations, and update the instruction as appropriate by September 2010.*

Recommendation 2.16: Assess Commanders' Need for Additional Authorities to Identify Indicators of Potential Violence in Civilian Personnel More Effectively

The Independent Review found that authorities governing civilian personnel are insufficient to support commanders and supervisors as they attempt to identify indicators of violence or take actions to prevent violence.

The Follow-on Review found that any attempt to grant commanders and supervisors greater authorities would not be consistent with the employee's civil rights and liberties. However, the Follow-on Review also found that more could be done to provide training on the prevention of workplace violence, and to enhance supervisors' and managers' visibility into the authorities available to them to address workplace behavioral issues with regard to civilian personnel.

- **Future Action on Identifying Indicators of Violence in Civilian Personnel:** The Under Secretary of Defense for Personnel and Readiness will work with civilian Employee Relation Component representatives to develop a DoD policy on prevention of workplace violence.

Civilian supervisor training will be promulgated as part of the revision of DoDI 1400.25, Volume 412 (*Civilian Leader Development*) by January 2011.

Recommendation 3.1 a-c: Improving Force Protection Policy

The Independent Review found DoD lacks a senior official assigned overall responsibility for oversight and integration of force protection policy across the Department. Instead, several different Senior DoD officials are responsible for issuing policy in force protection-related subject areas. Additionally, there is a lack of clarity regarding the force protection roles and responsibilities between Geographic Combatant Commanders and the Military Departments, especially in the United States. Finally, clarity on command and control responsibility for force protection is essential for a rapid response to multiple near simultaneous events similar to the Fort Hood incident.

During the analysis by the Follow-On Review, an additional finding was identified. DoD has a long-standing lack of a senior official responsible for overall oversight and integration of law enforcement activities. Force protection and law enforcement activities are overlapping. To the extent that the Department needs better force protection integration, DoD also needs better integration of law enforcement.

- **Future Action to Integrate Force Protection Policy:** The integration of force protection policy and law enforcement policy across the Department urgently requires a more senior level oversight structure than what currently exists. However, the current programs and policy offices are so diverse that assigning a single senior official would require a major restructuring within the Department. Therefore, the Senior Steering Group of the Follow-On Review chaired by ASD(HD&ASA) will assume an additional and separate duty as a standing departmental body to meet not less than biannually to address Department-wide policy synchronization and integration issues related to force protection and law enforcement activities. This force protection and law enforcement steering group will report to the Deputy Secretary of Defense Advisory Working Group following each meeting.
- **Future Action to Clarify Service and Combatant Commander Roles for Force Protection:** The Secretary of Defense will issue a guidance memorandum to DoD Components clarifying the force protection responsibilities and authorities of the Geographic Combatant Commanders and other heads of DoD Components. The memorandum will emphasize the need for Military Departments' compliance with force protection reporting requirements to the appropriate Combatant Commander.

Recommendation 3.2 a-c: Integrate Force Protection Efforts against Internal Threats

The Independent Review found DoD force protection programs and policies are not focused on internal threats. Recommendations included: develop policy and procedures to defend against insider threats, commission a multidiscipline study to examine and evaluate threat assessment programs, and provide commanders with a multidiscipline capability focused on predicting and preventing insider attacks.

- **Future Action to Integrate Force Protection Efforts:** The Under Secretary of Defense for Acquisition, Technology, and Logistics will commission the Defense Science Board (DSB)

to examine and evaluate existing training, procedures, reporting requirements/mechanisms, threat assessment programs, and best practices for identifying predictive indicators of pending violence and managing emerging insider threats. The Defense Science Board will complete its study by March 2011. The Fort Hood Follow-on Review Senior Steering Group will appoint a lead agency to draw on these findings to develop policy and procedures to improve and integrate DoD programs to defend resources and personnel against internal threats. The Under Secretary of Defense for Personnel and Readiness will incorporate the DSB findings and tools developed under recommendations 2.9, 2.12, and 2.13 to provide a multidiscipline approach against insider threats for commanders.

Recommendation 3.3 (a, b, c): DoD Joint Terrorism Task Force Participation

The Independent Review found that DoD's commitment to Joint Terrorism Task Forces (JTTFs) is inadequate. Issues include the lack of a single agency appointed to lead DoD's efforts in JTTFs, inconsistent memoranda of understanding between FBI and DoD that govern activities of the Department and DoD Agencies, and a possible under commitment or misalignment of DoD resources supporting JTTFs.

- *The Under Secretary of Defense for Policy (USD(P)) will serve as the DoD lead for oversight, providing policy guidance and developing DoD-wide goals and objectives for JTTFs collaboration. By September 2011, USD(P) will begin drafting and coordinating one consolidated Memorandum of Understanding (MOU) between the FBI and DoD, including the DoD Inspector General's Defense Criminal Investigative Service, to clarify responsibilities and ensure consistency among all agencies. This JTTF MOU will be developed within the context of a January 2009, White House-directed, Under Secretary of Defense for Intelligence (USD(I))-drafted, Information Sharing MOU between DoD and FBI (staffing began in June 2010). Finally, USD(P) will review personnel and data from a resource study provided by the USD(I) to ensure the commitment of resources to JTTFs meets DoD requirements. Resource and organizational requirements, including requests for additional manpower, will be determined no later than October 2010, and the realignment plan, if required, will be completed by October 2012.*

Recommendation 3.4: Develop Guidance on Force Protection Threat Information Sharing

The Independent Review found DoD lacks guidance standardizing how to share Force Protection (FP) threat information across the Services or the Combatant Commands. The Independent Review recommended standardizing guidance regarding how military criminal investigative organizations and counterintelligence organizations will inform the operational chain of command.

To ensure the development of coherent policies spanning intelligence, counterintelligence, law enforcement, and investigative jurisdictions, the Under Secretary of Defense for Policy (USD(P)) is given a more proactive role in this area.

- **Future Action on Force Protection Information Sharing:** USD(P) will direct the development of standard guidance regarding how Defense Criminal Investigative Organizations, Counterintelligence Organizations, and Intelligence Organizations will inform

the operational chain of command as well as keep the Joint Intelligence Task Force for Combating Terrorism (JITF-CT) and Services informed.

- By October 2010, the Under Secretary of Defense for Intelligence (USD(I)) will designate JITF-CT as the lead for facilitating selective access to foreign-connected terrorism-related information to designated organizations.
- By May 2011, USD(P), in coordination with USD(I) and the Assistant to the Secretary of Defense for Intelligence Oversight, will establish FP threat information dissemination policy and procedures for Defense intelligence collection, counterintelligence, and criminal investigative organizations in response to Combatant Commander, Service, and Defense intelligence analytical agencies' requirements.
- By November 2011, DoD Antiterrorism, FP, counterintelligence, intelligence, and law enforcement components will begin reviewing and updating policies, procedures, and training to comply with the new USD(P) policies.

Recommendation 3.5.a: Adopt a Common Force Protection Threat Reporting System

The Independent Review found that DoD did not have direct access to a force protection threat reporting system for suspicious incident activity reports. DoD agrees with this finding. In an August 2007 memo, the Deputy Secretary directed termination of DoD's only Force Protection Threat Information (FPTI) Reporting system, which was called the Threat and Location Observation Notice (TALON) reporting system. He further directed the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to propose a long-term solution for DoD suspicious activity reporting that ensures appropriate privacy protection.

- *After two years of analysis and a successful pilot program completed in June 2009, the Department has selected the Federal Bureau of Investigation's (FBI) eGuardian system for DoD unclassified threat reporting. The eGuardian system, which is FBI-owned and maintained, provides an unclassified, secure web-based, capability to report suspicious activity and will contribute to our overall force protection threat information structure. The eGuardian system will appropriately safeguard civil liberties, while enabling information sharing among Federal, State, local, and tribal law enforcement partners, including interagency fusion centers.*
- *The Under Secretary of Defense for Policy is establishing a plan and will issue policy and procedures for the implementation of the eGuardian system as DoD's unclassified suspicious activity reporting system. Use of eGuardian will begin no later than September 2010.*

Recommendation 3.5 b: Adopt a Common Force Protection Threat Reporting System

The Independent Review found that DoD lacks direct access to a force protection reporting system for suspicious activity reports. Recommendations included adopting a common force protection threat reporting system and appointing a single Executive Agent to oversee and manage the system.

The April 12, 2010 Interim Report addressed the first recommendation. This recommendation was implemented in May 2010, with the approval of using the eGuardian system. The

eGuardian system, which is FBI-owned and maintained, will incorporate appropriate safeguards for civil liberties, while enabling information sharing among Federal, State, local, and tribal law enforcement partners, including interagency fusion centers. DoD will begin using the eGuardian system no later than September 2010.

- **Future Action to Ensure Common Threat Reporting:** The Under Secretary of Defense for Policy (USD(P)) will recommend the appropriate management arrangement (e.g., Executive Agent or Lead Component) to the Deputy Secretary of Defense to implement and manage the Department's use of the eGuardian system by November 2010. USD(P) will incorporate those requirements within the final issuance governing *Law Enforcement Reporting of Suspicious Activity* by December 2010.

Recommendation 3.6: Create a Process for Sharing Real-Time Force Protection Event Information Among Installations

The Independent Review found that there are no force protection processes or procedures to share unclassified real-time event information among commands, installations, and components. In November 2009, Fort Hood, Texas went to Force Protection Condition (FPCON) Delta. There were no indications that the rest of the Continental United States DoD forces were immediately notified of the event. Most installations found out about the event through the news media. Events that are happening within one Area of Responsibility (AOR) should inform force protection decisions in another. The requirement for a process/system to share event information in near real-time is key for alerting the force that an attack is underway.

- **Future Action to Enable Real-Time Force Protection Information Sharing:** This recommendation is also being covered by new Secretary of Defense guidance to the Military Services and to Combatant Commanders under Recommendation 3.1. Additionally, the Joint Staff (JS) will evaluate the current incident reporting systems used by the National Military Command Center (NMCC) and update Chairman Joint Chiefs of Staff Manual (CJCSM) 3150.03C (*Joint Reporting Structure Event and Incident Reports*) or other appropriate CJCSM no later than April 2011. By January 2011, the Services will ensure that all organizations are trained in reporting systems used by the NMCC. By April 2011, Combatant Commands will ensure there is an unclassified means to notify all DoD facilities within their AOR of an FPCON change.

Recommendation 3.7 a, b: Review and Update Access Control Protocols to Detect Insider Threats

The Independent Review found that DoD installation access control systems and processes do not incorporate behavioral screening strategies and capabilities, and are not configured to detect an insider threat. DoD policy mandates 100-percent credentials inspection for access to DoD installations. A properly credentialed person has authorized access to an installation. Detecting a trusted insider's intention to commit a violent act requires observation of behavioral cues/anomalies. There are Federal programs that train personnel to observe individuals under routine conditions. These programs may be useful if employed by DoD security guards, police officers, supervisory personnel, and persons working in visitor control centers, or other common customer service contexts.

- **Future Action to Update Access Control Protocols:** DoD began reviewing best practices, technologies, procedures, and programs through the Physical Security Equipment Action Group-Defense Installation Access Control working group under the Deputy Assistant to the Secretary of Defense for Nuclear Matters. A feasibility analysis study on how behavior pattern recognition screening procedures and technology can detect anomalies of a potential insider threat will be completed by October 2010. The Office of the Under Secretary of Defense for Intelligence will review and assess the study findings by January 2011, and revise or develop policy guidance related to DoD 5200.08-R (*Physical Security Program*) or other DoD policies as appropriate by December 2011.

Recommendation 3.8: Review the Need for a DoD Privately Owned Weapons Policy

The Independent Review found that the Department does not have a policy governing Privately Owned Weapons. In the absence of such policy, the individual Services have established Privately Owned Weapons policies, which set minimum standards and task installation commanders to establish installation-specific requirements. These policies do not apply to personnel who live off installation.

- *The Under Secretary of Defense for Intelligence put into formal coordination a Secretary-issued Department-wide Interim Guidance Message. By early 2011, the interim guidance will be incorporated into a revision of DoD 5200.08-R (Physical Security Program).*

Recommendation 3.9 a-c: Develop Information Sharing Capabilities for Access Control to Installations

The Independent Review also found that the Services cannot share information on personnel and vehicles registered on installations, installation debarment lists, and other relevant information required to screen personnel and vehicles, and grant access. The Services do not have access to the National Crime Information Center (NCIC) or Terrorist Screening Database (TSDB) to obtain relevant information to screen visitors. The review also identified that automated systems should be able to authenticate against centralized authoritative databases on registered persons and share access control information among installations. This recommendation supports on-going efforts to survey installation and mission requirements and to coordinate and prioritize the use of automation to mitigate risk and threat.

- **Future Action to Share Information for Access Control:** Under existing DoD issuances, services are implementing automated access control capabilities that will enable authentication of various identification media against authoritative databases. Services will accelerate implementation of automated access control systems within resources constraints. Areas of acceleration may include, but are not limited to, improvements in enterprise architecture and technology associated with Physical Access Control System (PACS), improved access to law enforcement databases such as the NCIC or TSDB, and capabilities that enable information sharing across the DoD enterprise. A current Under Secretary of Defense for Intelligence (USD(I))-sponsored study of existing physical access control system capabilities and limitations, and a joint DOJ-DoD NCIC access test, will be completed by January 2011. USD(I) will evaluate and update physical security policy and issuances by December 2011.

Recommendation 4.1 a: Establish Milestones for Compliance with the Installation Emergency Management Program

The Independent Review found that the Military Departments are not fully interoperable with all military and civilian emergency management stakeholders. Additionally, some DoD installations have not implemented procedures that are consistent with the National Incident Management System (NIMS). DoD has instructed the Military Departments to develop Initial Operational Capability (IOC) by January 13, 2011, and to have Full Operational Capability (FOC) by January 13, 2014, for NIMS-consistent procedures. However, DoD guidance was unclear on what constitutes IOC and FOC consistency.

- *The Under Secretary of Defense for Acquisition, Technology and Logistics has issued interim guidance on tasks required for IOC and FOC, and initiated formal coordination of DoDI 6055.17 (DoD Installation Emergency Management Program).*

Recommendation 4.1 b: Assess the Potential for Accelerating the Timeline for Compliance with the Installation Emergency Management Program

The Independent Review found that Services are not fully interoperable with all military and civilian emergency management stakeholders. DoDI 6055.17 (*DoD Installation Emergency Management (IEM) Program*) directs the Services to adopt IEM programs consistent with the National Incident Management System (NIMS). The Under Secretary of Defense for Acquisition, Technology, and Logistics has instructed the Services to develop Initial Operational Capability (IOC) for IEM programs by January 2011 and Full Operational Capability (FOC) by January 2014.

To attain IOC and FOC, Services must implement a Common Operating Picture (COP) and Mass Notification and Warning Systems (MNWS). In addition, the Independent Review calls on Services to implement Enhanced 911 (E 911). The Independent Review recommends the Department assess the potential for accelerating the timeline for compliance with the IEM Program.

- **Future Action to Clarify Installation Emergency Management Program Requirements:** In June 2010, the Under Secretary of Defense for Acquisition, Technology, and Logistics initiated formal coordination of DODI 6055.17 (*DoD Installation Emergency Management (IEM) Program*) to clarify requirements for E 911, MNWS, and COP.
- **Future Action to Implement Installation Emergency Management Programs:** The Follow-On Review determined there is a need to implement certain IEM program elements as described below as soon as possible (see Recommendations 4.2, 4.4, and 4.5a).

Recommendation 4.2: Develop Policy to Implement Enhanced 911 Services

The Independent Review found that there is no DoD policy implementing public law requiring a 911 capability on DoD installations (Public Law 108-494, *Enhanced 911 Services*). The Independent Review recommended the Department develop policies that provide implementation guidance for Enhanced 911 (E 911) services. The two benefits of E 911 are that it automatically

notifies dispatchers of a caller's location, including cell phones, and that it has the capability to broadcast emergency notifications out to designated geographic locations. The two basic components of an E 911 capability are: (1) E 911 phone consoles that draw from a database that identifies caller location; and (2) trained dispatchers. Computer aided dispatcher systems contribute to a more sophisticated E 911 capability. Most civilian communities already have E 911 programs (funded through a national tax on phone services), but most DoD installations do not, because DoD installations were not part of the Congressionally mandated requirement.

- **Future Action to Implement Enhanced 911:** The Follow-On Review determined military personnel should receive the same emergency response services as their civilian counterparts. A DoD E 911 capability must be funded to meet Full Operational Capability (FOC), as outlined in DoDI 6055.17 (*DoD Installation Emergency Management (IEM) Program*), as soon as possible and no later than 2014. To meet FOC, E 911 systems should be commensurate with and supportable by E 911 systems in the surrounding local communities (or by comparable emergency notification systems in communities outside of North America). The Secretary places a high priority on this IEM program and directs the Services to work with Cost Analysis and Program Evaluation during the FY 2012-2016 Integrated Program/Budget Review to develop funding options to achieve FOC no later than 2014. Services should use the FY 2012-2016 Integrated Program/Budget Review process to determine how to prioritize and tailor IEM program implementation to maximize improvements to installation emergency preparedness using the minimum resources necessary, taking into account the unique requirements of installations of varying size and mission type.

Recommendation 4.3 a: Incorporate Law Enforcement Best Practices for Active Shooter Threat

The Independent Review found DoD does not currently take advantage of successful models for active shooter response for civilian and military law enforcement on DoD installations and facilities. More generally, the Department has no established process to identify and adopt quickly civilian law enforcement best practices. The Independent Review recommended the Department identify and incorporate civilian law enforcement best practices, including response to the active shooter threat, into training certifications for civilian police and security guards.

- **Future Action to Incorporate Best Practices:** In March 2010, DoD took several steps to specifically address the active shooter threat scenario. Moving forward, the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) will recast a joint Law Enforcement Training Standards Working Group to identify and incorporate a broad range of law enforcement best practices. By November 2010, USD(P&R) will update DoDI 5210.90 (*Minimum Training, Certification, And Physical Fitness Standards for Civilian Police and Security Guards (CP/SGs) In The Department of Defense*) or draft a new instruction accordingly.

Recommendation 4.3 (b, c, d): Develop Law Enforcement Practices for Active Shooter Threat

The Independent Review found that DoD policy does not currently take advantage of successful models for active shooter response, use the same minimum training standards for both civilian

and military law enforcement units on DoD installations, or incorporate Department of Homeland Security (DHS) best practices for workplace violence into DoD Antiterrorism Level 1 training. Responding officers at Fort Hood attributed their actions during the incident to a new active response training protocol instituted last year by the Fort Hood Department of Emergency Services.

Note: In March 2010, DoD incorporated a new training module addressing active shooter threats into the Antiterrorism Level 1 online training.

- *The Under Secretary of Defense for Acquisition Technology, & Logistics (USD(AT&L)) has updated and initiated formal coordination of DoDI 6055.17 (DoD Installation Emergency Management (IEM) Program). It directs commanders to incorporate the "Active Shooter" scenario, lessons learned from Fort Hood, and other workplace violence case studies into their Installation Emergency Management training programs. The Under Secretary of Defense for Personnel and Readiness has investigated the implementation of minimum standards for military police (and equivalents) and will draft a change to DoDI 5210.90 (Minimum Training, Certification, And Physical Fitness Standards For Civilian Policy And Security Guards (CP/SGs) In The Department Of Defense) or draft a new instruction by November 2010.*

Recommendation 4.4: Examine and Incorporate State-of-the-Art Mass Warning Systems into Emergency Response Plans

Based on Joint Staff Integrated Vulnerability Assessments, the Independent Review found that many DoD installations lack mass notification capabilities. The Independent Review recommended the Department examine the feasibility of advancing the procurement and deployment of state-of-the-art Mass Notification and Warning Systems (MNWS) and incorporate these technologies into emergency response plans. The purpose of MNWS is to provide warning and response direction for all personnel within 10 minutes of incident notification and verification. MNWS has four elements: (1) Giant Voice for outdoor areas; (2) Indoor Voice for indoor facilities; (3) Telephone Alert System for phone call/text alerts; and (4) Software Alert Systems for computer alerts. Depending on the installation, different combinations of components may be required to meet FOC for mass notification. All installations have some MNWS in place, but the systems are not robust. A state-of-the-art MNWS automates guidance (e.g., evacuation orders for certain areas) to help emergency responders manage a crisis.

- **Future Action to Implement Mass Notification Warning Systems:** The Follow-On Review determined there is a need to implement MNWS. Each Service should determine the combination of elements most appropriate to meet FOC requirements for mass notification. MNWS programs must be funded to meet Full Operational Capability (FOC), as outlined in DoDI 6055.17 (*DoD Installation Emergency Management (IEM) Program*), no later than 2014. To meet FOC, MNWS must notify all installation personnel within ten minutes of incident verification. The Secretary places a high priority on this IEM program and directs the Services to work with Cost Assessment and Program Evaluation during the FY 2012-2016 Integrated Program/Budget Review to develop funding options to achieve FOC no later than 2014. Services should use the FY 2012-2016 Integrated Program/Budget Review process to determine how to prioritize and tailor IEM program implementation to maximize improvements to installation emergency preparedness using the minimum resources

necessary, taking into account the unique requirements of installations of varying size and mission type.

Recommendation 4.5 a: Accelerate Deployment of Common Operating Picture Capability into Installation Emergency Operations Centers

The Independent Review found that Services have not widely deployed or integrated a Common Operating Picture (COP) capability into Installation Emergency Operations Centers (IEOCs) per direction from the Under Secretary of Defense for Acquisition, Technology, and Logistics. The Independent Review recommended the Department examine the feasibility of accelerating the deployment of state-of-the-art COP to support IEOCs. COP is a web-based software system and there are many commercially available software packages, such as Web-EOC and E-Team. COP enables coordination between emergency responders on- and off-installation, allowing them to share the exact same information in real time over the course of an incident. COP also improves installations' capacity to report force protection information to the Combatant Commands.

- **Future Action to Implement a Common Operating Picture:** The Follow-On Review determined installations require COP capability, particularly given its benefits to force protection and emergency management for a relatively low resource requirement. COP capability must be funded to meet Full Operational Capability (FOC), as outlined in DoDI 6055.17 (*Installation Emergency Management (IEM) Programs*) no later than 2014. To meet FOC, the COP capability must share real-time information among first responders. The Secretary places a high priority on this IEM program and directs the Services to work with Cost Analysis and Program Evaluation during the FY 2012-2016 Integrated Program/Budget Review to develop funding options to achieve FOC no later than 2014. Services should use the FY 2012-2016 Integrated Program/Budget Review process to determine how to prioritize and tailor IEM program implementation to maximize improvements to installation emergency preparedness using the minimum resources necessary, taking into account the unique requirements of installations of varying size and mission type.

Recommendation 4.5 b: Develop an Operational Approach that Sets Force Protection Condition Appropriately

The Independent Review recommended the Department develop an operational approach that raises the Force Protection Condition in response to a scenario appropriately and returns to normal while considering both the nature of the threat and the implications for force recovery and healthcare readiness in the aftermath of the incident.

- **Future Action to Set Force Protection Condition Appropriately:** The previous recommendation on creating a process for sharing real-time force protection event information among installations (3.6) addresses the development of an operational approach to raise Force Protection Condition. By April 2011, Combatant Commands will ensure there is an unclassified means to notify all DoD facilities within their AOR of an FPCON change.

Recommendation 4.6 a, b: Review and Establish Policies for Synchronizing Installation Emergency Management Procedures

The Independent Review found that DoD Installation Emergency Management (IEM) program stakeholders have not yet synchronized their applicable programs, policies, processes, and procedures. Better synchronization and coordination would remove redundant planning requirements, identify seams in policy, focus programmed resources, and streamline procedures to achieve unity of effort.

- **Future Action to Synchronize Installation Emergency Management:** The Follow-on Review developed a Policy Architecture Analysis. This Analysis recommended the Department publish a new Directive to synchronize IEM and related programs, policies, processes, and procedures across the Department. To address this recommendation, the Under Secretary of Defense for Policy has established a stakeholders working group, with the goal of placing draft synchronizing policy in coordination by January 2011.

Recommendation 4.7: Review Installation Emergency Management Programs to Ensure Appropriate Interaction with Mutual Aid Agreements

The Independent Review found that the Mutual Aid Agreements (MAAs) between DoD installations and civilian support agencies are not current and need to be updated. There is no overarching guidance regarding the maintenance, frequency of review, and tracking of MAAs. DoDI 6055.17 (DoD Installation Emergency Management Program) tasks installations to develop resource management objectives that address partnership agreements essential to Installation Emergency Management.

- *The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) has initiated formal coordination of DoDI 6055.17 to clarify oversight and exercise requirements, including annual reviews, integrating tracking, exercising, and inspections of MAAs.*

Recommendation 4.8.a: Develop Core Service Elements of a Family Assistance Center

The Independent Review found that lessons from the terrorist attacks in 2001 resulted in sufficient policy guidance for implementing day-to-day support programs and baseline family support services. However, the policy guidance has not been updated nor does it clearly delineate a specific structure for how these services integrate in support of a crisis or mass casualty incident. As a result, Military Department-level planning lacks consistency and specificity, which leads to variation in the delivery of victim and family care.

- *The Under Secretary of Defense for Personnel and Readiness reviewed the Pentagon 9/11 After Action Report and all applicable Military Department regulations, and identified best practices that will be incorporated into the draft revision of DoDI 1342.22 (Family Centers) by December 2010.*

Recommendation 4.8 b, c: Develop Core Service Elements of a Family Assistance Center

The Independent Review found that the Department of Defense has not produced guidance to develop family assistance plans for mass casualty and crisis response. As a result, Service-level planning lacks consistency and specificity, which leads to variation in the delivery of victim and family care.

- **Future Action to Develop Family Assistance Centers:** In June 2010, the Under Secretary of Defense for Acquisition, Technology, and Logistics initiated formal coordination of DoDI 6055.17 (*DoD Installation Emergency Management (IEM) Program*) to ensure Family Assistance Center crisis and mass casualty response plans become integral elements of the IEM program. The Family Assistance Center crisis and mass casualty response will “establish procedures to integrate victim and family services in response to the full spectrum of crisis or catastrophic events.” The Under Secretary of Defense for Personnel and Readiness will review and identify Service best practices and revise DoDI 1342.22 (*Family Readiness Program*) to incorporate a best practices model for a family assistance center by December 2010.

Recommendation 4.9 (a, b): Ensure Religious Support in Mass Casualty Incidents

The Independent Review found no comprehensive instructions that address religious support, planning, or integration requirements in response to a mass casualty incident. This results in inconsistencies in Military Department policies on integrating religious support into emergency management, and could lead to inadequate planning and coordination for religious support resources.

- *The Under Secretary of Defense for Personnel and Readiness, with the advice and assistance of the Armed Forces Chaplains Board and the Armed Forces Chaplains Center, reviewed Military Department policies and civilian sector programs and identified best practices for religious support to mass casualty incidents. USD(P&R) will begin to update guidance for policy additions or revisions to applicable policy governing installation emergency management and response to disasters or incidents by September 2010.*

Recommendation 4.10: Review Mass Casualty Incident Response Training in the Chaplain Basic Officer Courses

The Independent Review found inconsistencies among Military Department entry-level chaplain training programs, which can result in inadequate religious support during a mass casualty incident. The newly established Armed Forces Chaplaincy Center (AFCC) is comprised of the Army, Navy, and Air Force Chaplain Schools. The Department will obtain advice from the AFCC and the Armed Forces Chaplains Board on an optimal manner of introducing mass casualty incident training into the basic course and/or other training opportunities for newly commissioned chaplains can develop enhance counseling and care skills consistent with their knowledge, skills, and abilities.

- *The Under Secretary of Defense for Personnel and Readiness has put into formal coordination DoDI 6055.17, which will require that new chaplains get mass casualty incident training at the earliest point.*

Recommendation 4.11: Develop Standardized Policy Guidance on Memorial Service Entitlements

The Independent Review found that DoD has not published guidance regarding memorial service travel and transportation benefits authorized for certain survivors of deceased service members enacted in section 631 of Public law 111-84, the national Defense Authorization Act for Fiscal Year 2010. DoD guidance is necessary to ensure this benefit is administered consistently throughout the Department.

- *The Under Secretary of Defense for Personnel and Readiness established interim guidance (DTM 10-008 – Travel and Transportation for Survivors of Deceased Members of the Uniformed Services to Attend Memorial Ceremonies) and will incorporate its content into the pending revision of DoDD 1300.22 (Mortuary Affairs Policy), which will be published as a new DoDI with the same title, Mortuary Affairs Policy, during calendar year 2010.*

Recommendation 4.12 a, b: Review Mortuary Affairs Policies for Application to Private Citizens within the Continental United States

The Independent Review found that DoD and Service casualty policies revealed no guidance, at any level, that was sufficient to address the full range of issues pertaining to private citizens who become casualties on a CONUS military installation. In the area of DoD and Service mortuary affairs policies, the review revealed a similar absence of guidance regarding mortuary entitlements and services.

- **Future Action to Update Mortuary Affairs Policies:** The Under Secretary of Defense for Personnel and Readiness will coordinate with the Defense Human Resource Activity Law Enforcement and the Office of the Assistant Secretary of Defense for Health Affairs to establish policy and draft guidance to revise DoDI 1300.18 (*Department of Defense (DoD) Personnel Casualty Matters, Policies and Procedures*), DoDI 1300.22 (*Mortuary Affairs Policy*), and other applicable issuances no later than September 2010.

Recommendation 5.1 a-c: Optimize Mental Healthcare for Domestic Mass Casualty Incident

The Independent Review found that DoD installations have not consistently planned for mental health support after domestic mass casualty incidents for victims and their families. Current DoD medical policy regarding combat stress does not specifically address an appropriate traumatic stress response in a domestic mass casualty incident. Several DoD programs and initiatives are currently working to address this shortcoming.

- **Future Action to Optimize Mental Healthcare:** The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) completed a review of existing policies, guidance, and evidence-based practices inside and outside of DoD, and, in June 2010, recommended

the development of a DoDI on post-disaster mental health response. USD(P&R) will draft and place into coordination interim guidance on disaster response strategies by December 2010.

Recommendations 5.2 (a, b, d): Create Policies to Measure Health Care Provider Readiness

The Independent Review found that the Department does not endorse a program encompassing all of the desired attributes of a health care provider readiness strategy. Although the Independent Review found the Department has evolving collaborations between DoD entities and civilian organizations to support health care providers, it suggested that DoD should further develop formal collaboration relationships with the civilian sector to share best practices and ongoing research outcomes.

Note: This finding is partially approved for parts “a” and “b” because the necessary policies to ensure health care provider readiness already exist. They are not, however, fully integrated and current.

- *The Under Secretary of Defense for Personnel and Readiness will review existing policies and guidance, establish a Directive-Type Memorandum related to civilian resiliency resources, and update and integrate policies as necessary by September 2010.*

Recommendation 5.2 c: Create Policies to Measure Health Care Provider Readiness

The Independent Review found that DoD does not have comprehensive policies that recognize, define, integrate, and synchronize monitoring and intervention efforts to assess and build health care provider readiness. DoD does not have readiness sustainment models, with requisite resources, for the health provider force that are similar to readiness sustainment models for combat and combat support forces.

The Follow-on Review found that DoD does have readiness sustainment models inclusive of health care providers. However, the demand for support from caregivers in general, and from mental health care providers in particular, is increasing and appears likely to continue to increase due to the stress on military personnel and their families from our high operational tempo and repeated assignments in combat areas.

- **Future Action to Assess and Build Health Care Provider Readiness:** In accordance with approved recommendations from the Follow-on Review’s Interim Report, the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) is currently conducting a review of existing policies, guidance, and current initiatives/programs that specifically target health care providers, especially mental health providers, to evaluate their content, and will draft and place into coordination updates by September 2010. Based on the results of the review, by November 2010 USD(P&R) will also prepare the business case for additional mental health providers, specifying the number of providers needed as well as the resources required to reach that number of providers. In accordance with the business case, USD(P&R) will then develop new policies to assess and build health care provider readiness.

Recommendation 5.3 (a, c): Ensure Integrated Policies to Sustain High Quality Care and De-stigmatize Health Care Providers Who Seek Treatment

The Independent Review found that increasing demands on health care support will make it difficult to sustain high-quality care due to the high operational tempo and work-related stress on caregivers. The Department needs to develop a deployment model that provides sufficient recovery and sustainment for health care providers, and de-stigmatizes health care providers who seek treatment for stress. DoD also needs to integrate the existing body of policies, processes, procedures, and programs to ensure consistency and a comprehensive approach.

- *The Under Secretary of Defense for Personnel and Readiness will review and update existing policies and guidance, to ensure they are integrated and provide appropriate guidance to sustain high quality care, and complete the conversion of an anti-stigma DoDI based on DTM 09-006 (Revising Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Military Personnel), by September 2010.*

Recommendation 5.3 b: Ensure Integrated Policies to Sustain High Quality Care and De-stigmatize Health Care Providers Who Seek Treatment

The Independent Review found that the lack of a readiness sustainment model for the health provider force, the unique stressors that healthcare providers experience, and the increasing demand for support combine to undermine force readiness. The Independent Review recommended that DoD develop integrated policies, processes, procedures, and properly resourced programs to sustain high quality care.

The June 2007 Report of the DoD Task Force on Mental Health noted the importance of enhancing the resiliency and recovery of combatants due to the emotional pathology of combat. The Services have robust programs for pre- and post-deployment care for their members, but some have only recently initiated similar programs for healthcare providers. It is equally important to enhance the resilience and recovery of healthcare providers.

- **Future Action to Support Health Care Providers:** The Under Secretary of Defense for Personnel and Readiness developed a strategy to enhance resilience that addresses the total health and comprehensive well-being of healthcare providers. It accounts for various factors, including deployment length, post-deployment reconstitution, and dwell time, and assesses the advantages and disadvantages of using temporary providers to fill shortfalls. The strategy incorporates a new resilience model, which will be drafted and placed into coordination by September 2010.

Recommendation 5.4: Provide Mentor Relationships Among Healthcare Providers

The Independent Review found that senior caregivers are not consistently functioning as clinical peers and mentors to junior caregivers. It also raised concerns regarding the retention rate of experienced physicians. The Independent Review recommended a review of Senior Medical Corps officer requirements to determine optimal roles, utilization, and assignments.

The Follow-on Review found that current assignment processes in the Medical Departments of each Service are unique to the specific mission requirements of each Department, and are already responsive to those requirements.

- **Future Action to Improve Mentoring:** The Army, Navy, and Air Force will maintain the current assignment process developed by each Service, and expand them as they deem necessary to ensure that Senior Medical Officers are assigned to clinical positions.